10.71 Release Summary

iOS / macOS MDM

Disown device Web Services API

MaaS360 adds Disown Device Web Services API for Apple Device Enrollment Program (DEP) to support Apple feature of disowning or device removal process. The Disown Device API when invoked, disowns a device (based on device identifier) that are associated with the DEP token.

Note: After disowning a device, it needs to be manually removed control to un-enroll the device.

The API is used to disown devices and informs Apple's servers that the server no longer owns one or more MaaS360 enrolled DEP devices. The response that is obtained from the API is depicted as follows.

Success-Device is successfully disowned.

Not accessible-A device with the specified device ID is not accessible.

Failed-Disowning the device failed for an unexpected reason. Note: If 3 retries fail, then you need to contact Apple Support.

Support for configuring certificate based authentication for web pages by using Persona Policy

Maas360 adds support for enabling certificate-based authentication for web pages. The setting is listed under Browser Defaults in Persona Policy. On enabling this setting, allows user to authenticate to webpages by using an identity certificate. In the setting, choose the template ID for certificate authentication such as CE certs template id and derived credentials that is to be presented to the webpage when challenged. The setting is supported on MaaS360 iOS Browser 2.6+.

Android

One-stop shop for all Android enrollments >>

Maas360 adds Android Enrollment Wizard, a consolidated workflow for all Android enrollments - Device Admin, DO (Device Owner), and (PO) Profile Owner. The enrollment wizard displays interactive options to help you drill down to the Android enrollment method that suits your requirements. While this new feature greatly minimizes the time and efforts for the new customers, the existing Android enrollment menus are still available in the MaaS360 portal.

Deprecation of Device Admin policies >>

When the Android upgrades its OS to version 10 in 2019, some of the Device Admin policies will be deprecated.

Support for additional Android Enterprise policies >>

MaaS360 adds support for additional Android Enterprise policies for Android devices running OS version 9 and above.

App wrapping enhancements >>

MaaS360 adds support for new configuration parameters to overcome issues during the app wrapping. Effective 10.71, MaaS360 allows administrators to enable multidex for Analytics-only (marked for collecting analytics data) apps.

App Management

Support to add Android Enterprise apps from managed Google Play account >>

MaaS360 embeds managed Google Play iframe in the App Catalog to allow the administrators to add and approve Google apps directly from the managed Google Play store. In the previous releases, administrators had to add apps from the public Google Play store.

Support to edit app installation and update settings for Android enterprise apps >>

MaaS360 adds support to allow the administrators to edit the installation and update settings for Android enterprise apps. With this support, administrators can deploy the enterprise app updates to the devices that already have the primary version sideloaded through a third-party source (other than

MaaS360). Requires MaaS360 for Android agent 6.40 and above.

Support to stop or retry installation >>

MaaS360 adds a new Manage Distribution page to allow the administrators to track all the distribution targets of an app. With this feature, administrators can easily stop an active distribution and retry the installation if the installation of iOS apps is not successful. In case administrators have not used the **Number of times to retry** option while adding the app, they can still do a retry on-demand using the retry install feature. The retry installation feature is applicable only for iOS app distributions marked for instant install.

Windows

Support for Windows 10 Delivery Optimization (DO) policy setting >>

MaaS360 extends Windows 10 policy setting to support the Delivery Optimization (DO) method that is a peer-to-peer delivery of updates to an organization's networked PCs. The updates include Windows updates, security updates, Windows Store Apps, and Windows Store for Business Apps. By using the policy setting, select the peers included in the DO method, cache settings, and bandwidth throttling settings. The DO method addresses and reduces the bandwidth issues during the update process. The **Delivery Optimization** setting is accessible under Device Settings in a Windows policy setting.

Display of supported OS versions for any Windows MDM policy settings >>

MaaS360 displays the Windows OS version on which a specific Windows MDM policy setting is supported. The supported versions are displayed in the MaaS360 portal against the settings in the Windows policy. Some of the supported OS versions that are displayed are Windows Phone 8+, Windows 10 Professional, Education, Enterprise, Windows Team, and Windows Holographic.

Deep Links for Download and Install>>

MaaS360 adds an enhancement to the deep links feature in the Enterprise App Catalog. Previously users could navigate to a detailed view of an app in the Enterprise App Catalog by tapping a URL from a different app or from a web portal. Now, users can directly download and install the app from the provided link with just that one click. This feature is available on Windows 10+ MDM devices.

Default syntax to download and install an app: maas360appcatalog://launchapp?appID=77a5f49b-3d10-3c1f-a073-8eca625dba2d&appVersion=1&downloadinstall=true

Note: Requires Windows Core 4.00, Windows MES 2.00

Support for WiFi SSID based Geofencing for Windows 10 MDM devices >>

Maas360 enhances the Geofencing feature to include WiFi based geo-fencing for Windows 10 MDM enrolled devices. The managed WiFi locations can be added in the Maas360 portal by administrators. To add a location login to the MaaS360 portal, and under **Security > Locations > Add Wi-Fi Locations**, enter the Location Name, Wi-Fi SSID and MAC Address. Administrators can enforce different policies based on whether the devices have Checked In to the managed WiFi locations. In order to do this, use "Assign Policies" action available for each managed location to assign an Windows 10 MDM policy to a device checking into managed location.

MaaS360 Portal also provides Checked In or Checked Out status of the devices getting connected or disconnected to those WiFi locations time to time. Users can also view the managed WiFi locations in the Windows 10 MaaS360 app on the device.

Note:

- Require MES Agent version 1.85, MaaS360 Core app 4.00.
- This feature is not available for self service. Contact IBM support to enable the feature.

Support to distribute Java Patches from Maas360 Portal >>

Maas360 automates and simplifies **Java patch handling** using custom Enterprise Patch Repositories that are administered from the MaaS360 portal with a one-click button. Enterprise Patch Repository definition does not require visibility into missing Java patches, but it is required to deploy and manage patches to users — on and off the corporate network, this is because Oracle mandates its customers to submit enterprise license for download and distribution of Java patches.

To distribute Java Patches, download them from the Oracle Website using your Oracle Enterprise License and host them on a server that is publicly available and it can serve as Enterprise Patch Repository server. Provide the server URL for Enterprise Patch Repository server under **Security> OS Patches (Windows) > Enterprise Patch Repository** to complete the setup.

IBM Cloud Identity support for Windows 10 Laptops and Desktops >>

MaaS360 adds Windows 10 Desktops and Laptops to the supported devices list that integrates with IBM Cloud Identity, a stand-alone identity service from

IBM, to provide single sign-on (SSO) capabilities that ensure only trusted devices and apps can access enterprise or corporate resources.

This provides easy SSO to native applications, Store apps, SaaS or web-based applications to boost productivity. It also provides conditional access to ensure that only trusted devices and applications access enterprise resources and two-factor authentication to mitigate risk of unauthorized access, saving the need to store multiple username/password. Previously the feature supported mobile devices with iOS 7+ or Android 5 and above.

Platform

Web Services API documentation availability from within the MaaS360 portal >>

MaaS360 allows administrators to access the web services API documentation from within the MaaS360 portal user interface. The user interface includes reference about the web services API, and an option to try out the APIs depending upon the type of access rights the administrator account has.

New compliance use cases under Business Templates based policy

MaaS360 enhances Business Templates based policy by introducing two more business use case templates. Center of Internet Security (CIS) and Security Technical Implementation Guide (STIG) business use case templates are listed for Business Templates based policy as part of Add Policy workflow. With this feature, you can create policy based on CIS and STIG security compliance templates-based policy.

New search attribute introduced for Advanced Search based on operating system OS version (numeric) >>

MaaS360 adds support for a new search attribute in Advanced Search that is based on operating system, called "OS Version (numeric)". ***Equal To, Greater Than, Greater Than or Equal To***, ***Less Than***, ***Less Than or Equal To***, and ***Not Equal To*** conditions are supported for this attribute.

The new search attribute is applicable for iOS, Android, Windows, macOS, and Windows Phone operating system. The OS version (numeric) attribute based search condition works for AND operator with platform name as the other condition. The search results return empty set for OR and other advanced search conditions.

Viewing Policy and Organization Profile Information for Policies >>

Maas360 adds an information section to the policies for administrators to check the origin of a policy. MaaS360 has policy recommendation engine which can suggest policies based on peer best practices. These community-based policies are derived using the variables of industry, device count and region, which is called as the organization profile. MaaS360 also has pre-defined policies based on business use cases.

The information section shows admins the organization profile that was chosen while creating a community-based policy, or for a business template based policy, it shows the business use case that was selected. The information is captured and shown for new policies created after 10.71 release. For existing policies, you can view the name and description of the policy in the information section. The organizational profile information is also displayed before publishing a policy with cognitive policy recommendations. The profile cannot be edited so that the recommendations are consistent whenever you edit a policy. A new policy can be created for a new profile or a new business case.

Password Prompt Controls for MaaS360 Portal >>

MaaS360 introduces controls for password prompt that is displayed to administrators when they take important actions on the portal. The password prompt is to ensure that only authorized personnel take actions on the portal. MaaS360 recommends that the prompt should be always shown to all administrators. There are three settings available and the setting are configured based on the available administrator roles:

The option is available under **Setup > Administrators > More > Administrator Settings** .

- Prompt Always: Administrators are always prompted for password wherever applicable.
- Let Administrator Choose: Administrator can turn off password prompt for 5, 10, 20 minutes or rest of the session. If logged out they are prompted again, the next time.
- Never Prompt: Administrators are not prompted for a password for any action on the portal.
- If nothing has been set for a role, the default will be 'Prompt Always'.

Note:

- The settings are applicable from the next login to the MaaS360 Portal.
- All actions on the portal may not require password confirmation.
- The password prompt settings can be modified only by global administrators with Service Administrator role.

Importing specific user groups for an Azure AD tenant into the MaaS360 Portal >>

MaaS360 now allows administrators to import specific user groups for an Azure AD tenant into the MaaS360 Portal and synchronize data for these groups with existing groups in the MaaS360 Portal. This feature is available in the Master Admin Portal as the Enable Azure Group Based Data Sync custom property

Cloud Extender 2.96 and Mobile Enterprise Gateway (MEG)

New Cloud Extender Configuration Tool >>

For the MaaS360 10.71 platform release, the new Cloud Extender Configuration Tool is generally available for all customers. The Knowledge Center content will be gradually updated for the new tool in future MaaS360 platform releases.

Testing the validity of SSL certificates in the MEG trust store >>

The new Cloud Extender Configuration Tool provides a diagnostic tool that allows an administrator to check the validity of SSL certificates in the MEG trust store.

Testing the reachability of a WebDAV Fileshare or folder from MEG >>

The new Cloud Extender Configuration Tool provides a diagnostic tool that allows an administrator to test whether a WebDAV resource is reachable on the network.

10.70 Release Summary

iOS / macOS MDM

Web-apps support for iOS Home Screen Configuration

MaaS360 extends support for adding web-app to your iOS 12.0+ device home screen by using Home Screen Configuration from Policies page. Previously, only App and Folder configuration from Home Screen page was supported.

Support for Provider Type and Bundle Identifier for F5 Access VPN Profile >>

MaaS360 introduces the following enhancements:

- Provider Type for per-app VPN that supports App Proxy and Packet Tunnel provider types. For iOS 12+ devices, the provider type must be Packet Tunnel for the per-app VPN to work.
- Bundle Identifier is introduced for the VPN payload through which the administrator can provide the app bundle identifier of the VPN app in case the VPN vendor provides two different apps. **Note**: The Provider Type and Bundle Identifier option is available now for Palo Alto, Aruba, Sonicwall, Juniper, and CustomSSL VPN profile types that are supported in MaaS360.
- For F5 VPN Profile, MaaS360 introduces a new VPN type named as F5 Access and F5 SSL VPN is renamed as F5 Access Legacy. F5 Access supports the new iOS VPN framework that was introduced by Apple in iOS 10.3. An MDM profile with F5 Access works on devices that are iOS 10.3+ with the F5 Access app. The F5 Access Legacy configuration does not work from iOS 12.0 devices.

iOS policy Supervised settings >>

MaaS360 introduces following new Supervised settings under Restrictions & Network.

1. **Allow Date and Time Modification in iOS policy**: If enabled, users are allowed to change the date and time on the iOS device. The restriction is supported for iOS 12.0+ devices and is enabled by default. To restrict users from editing date and time on the iOS device, disable this setting and publish the policy to the device.
2. **New Supervised setting that is named as Allow Proximity Setup to New Devices**: If enabled, allows proximity setup for nearby devices. The device with this policy published allows proximity setup on nearby devices and setup by using the same Apple ID as in device with proximity setup policy enabled. The action is same as More > Wipe > Disable proximity setup on next reboot for a selected device from Device Inventory. In this release, the action is extended to Supervised devices by using Supervised settings in iOS policy. The restriction is supported for iOS 11.0+ devices.
3. **Allow USB Accessories while Locked:** If enabled, allows the device to make USB connection to accessories while the device is locked. The setting is enabled by default in the policy setting and allows USB accessories on the device when it is locked. The restriction is supported for iOS 11.3+ devices.

MaaS360 introduces following new Supervised settings under Notifications to disable selected notifications on iOS 12.0+ devices.

1. **Disable Notifications in CarPlay**: The notifications on the device are disabled during CarPlay mode. By default, the setting is enabled in the iOS policy. The restriction is supported on iOS 12.0+ devices.
2. **Enable Critical Notification**: If enabled, an app can mark the notification as a critical notification on the device by overriding Do Not Disturb and device ringer settings. By default, the setting is disabled in the iOS policy. The restriction is supported for iOS 12.0+ devices. Refer to summary of iOS 12 and macOS 10.14 day zero support here.

Skip setup of items during Profile configuration in Device Enrollment Program >>

MaaS360 adds iMessage and FaceTime options in Device Enrollment Program (DEP) Skip Items during Profile configuration for iOS devices. On enabling this option, iMessage and FaceTime is not shown to users for setup during iOS DEP enrollment. The function is supported for iOS 12 devices and for China only.

Android

Set up Android Enterprise during Quick Start >>

MaaS360 adds Android Enterprise to Quick Start, allowing the administrators to easily set up Android Enterprise during the startup.

Support for new Android Enterprise policies >>

MaaS360 adds support for additional Android Enterprise policies.

Support for new Device Admin security policies >>

MaaS360 adds support for additional M3, Kiosk, and Bluebird policies.

Support to send identity certificates from Cloud Extender to devices via MaaS360 portal >>

MaaS360 adds support to send individual identity certificates from Cloud Extender to the devices via Android MDM policies in the MaaS360 portal. The authorized third-party apps can use the identity certificates to authenticate users against those apps on the devices. Note: Contact MaaS360 support team to enable this feature for your account.

Beta - Google device attestation during Android Enterprise enrollments >>

Google mandates SafetyNet Attestation during Android Enterprise enrollment (DO and PO) to ensure that the devices pass Google's compatibility and integrity checks. Any device that fails attestation during the enrollment will not be able to complete provisioning. The status of the Google's SafetyNet device attestation is displayed in the detail view of the device. Previously, the SafetyNet Attestation was performed after the device enrollment. Note: Contact MaaS360 support to enable this feature for your account.

Manage restrictions on outgoing emails sent to external domains >>

MaaS360 adds support to allow administrators to enable restricts on outgoing emails sent to external domains. Based on the type of restriction, the outgoing emails to external domains are either blocked or a warning message is displayed.

Support for advanced wrapping features >>

MaaS360 revamps app wrapping features as per Android's recommendations.

Prompt for device name during Zero-touch enrollment and QR code for work-managed device enrollments >>

MaaS360 now supports a new configuration option that allows users to set a custom device name for the device that enrolls via Zero-touch (KME + DO, non-Samsung + DO) and QR code for work-managed device enrollments.

Windows

Support for BitLocker Device Encryption on Windows Pro devices >>

MaaS360 extends BitLocker encryption support for Windows 10 Pro devices. Previously, the feature was limited to Windows 10 Education and Enterprise editions. **Note**: The existing customers must re-publish the "Require Device Encryption" BitLocker policy on Security policies section to enforce them on Windows 10 Pro devices. Requires MDM Extender agent version 1.90 and Core app version 3.90. The BitLocker Drive Encryption feature is not supported on Windows Home edition.

Backup BitLocker Recovery password >>

MaaS360 also adds new policies to allow the administrators to backup the BitLocker recovery password to Active Directory (On-Premises or Azure) and MaaS360 End User Portal (EUP). The organizations that enforce BitLocker encryption through channels other than MaaS360 can also use these policies to backup the BitLocker Recovery password on the managed Windows 10 devices.

Device wipe action not supported on MDM enrolled Windows 10 devices below RS3

Due to limitations with Microsoft API in being able to support Wipe action on lower Windows 10 versions, MaaS360 has restricted the device wipe action to the Windows 10 OS version Redstone 3 (RS3) or 1709+. If the Windows 10 OS version is below RS3, the wipe action is not pushed to the device from the MaaS360 portal. Note that this will not affect devices that are enrolled via DTM enrollment method. To view the OS version, navigate to the detail view of the device > Hardware & OS tab > OS version. The OS version is displayed in 10.x.y.z format. The device wipe action is supported on OS versions where y > 15063. If the device wipe action is failed, the status can be tracked in the device history.

Minor usability improvement in Windows 10 enrollment

MaaS360 web-based enrollment for Windows 10 retained the enrollment start screen for the user after enrollment was completed, creating an impression that the enrollment was not completed. With this release, after the enrollment is initiated, the enrollment start screen in the Edge browser is automatically closed.

Removal of local administrator privileges on enrolled Windows 10 devices >>

Microsoft requires that the user accounts enrolling in MDM needs to necessarily have local admin rights on the Windows machine. MaaS360 adds a workaround to overcome this limitation for organizations, allowing the users to enroll the Windows 10 devices into MaaS360 without local admin privileges. **Note**: Some apps that require administrator privileges may not install or function.

Support to receive text notifications about policy changes >>

MaaS360 adds support to receive text notifications on the device whenever administrators enforce new policies or update existing policies. Note: Contact MaaS360 support to enable this feature for your account.

App Management

Deep links for MaaS360 enterprise app catalog >>

MaaS360 adds support for deep links, allowing the users to directly navigate to the detailed view of an application in the enterprise app catalog by just tapping an URL from a different app. For example, an IT administrator can create and distribute a custom URL pointing to the download page of a VPN application.

Viewing distributed apps and their status >>

Administrators can now view the status of the web apps / web clips distributed to an Android user from “App Distributions” tab on device view. Previously, this feature was available for iOS devices only.

Platform

Viewing Audit History in Settings >>

Maas360 All adds a new feature for global administrators with service admin roles to track and view history for any changes made in settings. The feature will track the history of Settings post 10.70 release.

Revamping the user interface of Expense Management View >>

Maas360 has a revamped the look and feel of the Expense Management view to get in tune with new UI of the portal. Expense Management will continue to define, manage and set alerts for the data usage of the Enrolled device with an added sort and filter feature.

Adding Salesforce Self-Serve link in the Help menu

Maas360 now enables a one-click link for Salesforce Self-Serve in the Help menu. It would be visible to customers who have Salesforce Self-Serve enabled.

Platform Administrators

Policy recommendation for Administrators

On creating a new Community Based policy, organization profile details that are provided during policy creation such as Industry, Region, and Deployment Size are retained and policy recommendations are suggested based on the profile that is selected during policy creation. Previously, the recommendations were based on customer profile detail that is available in MaaS360.

For existing policies that were added before 10.70 release, the recommendations continue to be based on customer profile that is available in MaaS360 for Industry, Region, and Deployment Size. The function is applicable for iOS, Android, and Persona policy. Note: macOS and Windows platforms do not support Community Based policy.

Clearing device location information based on Privacy Settings >>

Based on Privacy Settings to restrict location information, device location is cleaned up for devices that belong to the applicable ownership and group type that is mentioned in Privacy Settings. The historical location information is cleared up from the MaaS360 portal for these devices. The setting is applicable for all device types and device groups where location information for the device is supported.

Restricting device enrollment based on IP address within the corporate network >>

Configure Restrict Enrollments by IP setting from Advanced Device Enrollment Settings page to restrict device enrollment or activation by using IP ranges or IP addresses specified in the setting. The administrator can configure one or more allowed IP ranges and IP addresses for allowing device enrollment within the corporate company network. The IP address that is specified must be the final IP address from which request reaches MaaS360 servers. If using VPN, or proxies, the administrator needs to configure the final IP address in the allowed range. Contact IBM MaaS360 Customer Support team to get access to this setting.

The feature works for self-enrollment requests by users and enrollment requests that are created by the administrator. The IP address based enrollment support is not yet available for enrollment programs such as Apple Configurator, Device Enrollment Program (DEP), and license based Windows and Mac enrollments.

Manage Custom Attributes based on Rule Set

Based on custom attribute rules configuration, if for a device custom attribute value is anything apart from the allowed value that is configured in Rule Set then, the device is marked as Out of Compliance (OOC). This rule is applicable to 'Not Equal To' and 'Does Not Contain' conditions. Even if no custom attribute value is configured in the ruleset, the device is marked as Out of Compliance. Previously, any device with custom attribute "Compliance" value as null

for the enrolled device would not be marked as Out of Compliance (OOC).

Example: Consider custom attribute rule in Compliance Rules > select a rule set name > Custom Attribute Rules. Include custom attribute that is named as *testcustom*, Configure the rule for *testcustom* as Not Equal To 1. When this ruleset is applied on the device, any device whose custom attribute value is anything apart from one or if not configured then the device is marked as Out of Compliance.

Analytics

Show count of mitigated insights in the My Advisor notification email

MaaS360 sends My Advisor notification email to administrators who subscribe to it for Insights. This notification email now includes the count of insights that were mitigated in the previous week. If a risk insight is relevant to the customer and later the impacted device count is reduced to zero, it is referred as a 'mitigated insight'.

Cloud Extender 2.95

Zebra Printer Management module >>

MaaS360 introduces a new module for Cloud Extender that allows administrators to remotely manage configuration settings and take actions on Zebra printers that are discoverable on the corporate network. **Note:** This module is supported for the MaaS360 platform 10.70 release only and requires Cloud Extender 2.95 and the new Cloud Extender Configuration Tool. Contact IBM Support to enable this setting.

10.69 Release Summary

iOS / macOS MDM

Push iOS update to a device, Device Groups, User Groups >>

In Push iOS Update, an option is added to download and install the latest iOS OS version that is available for a specific device, Device Groups, and User Groups for devices enrolled in MaaS360.

Support for uploading multiple MobileConfig files from iOS and macOS policy settings >>

MaaS360 extends support to add multiple MobileConfigs files for iOS and macOS devices by using iOS and macOS policy settings. Previously, MaaS360 supported adding only one MobileConfig file from policy settings. Customers can add multiple payloads in the MobileConfig files by creating any new MobileConfigs as needed.

Publishing Identity Certificate from Cloud Extender to devices from Certificate Credentials policy setting >>

MaaS360 extends support to send Identity Certificates to the devices individually to the device keychain for iOS and macOS devices. To support this capability, MaaS360 introduces configuration of Identity Certificate from Certificate Credentials in Policy settings. Contact IBM MaaS360 Customer Support team to enable Identity Certificate credentials setting for your customer account.

Configure Active Directory account for macOS device by using policy setting >>

MaaS360 supports Active Directory configuration in User Settings under macOS policy. On publishing the policy, Payload with Active Directory settings gets installed on the device.

App addition status and license information for auto uploading of Volume Purchase Program apps >>

MaaS360 introduces new attribute App Addition Status in the Volume Purchase Program (VPP) page that displays the auto upload status for a VPP token. Additionally, View option is introduced for every VPP token name that is listed in the VPP page that guides to the VPP Token Details page. For a VPP token, all iOS apps that are associated with the token with license information, auto app addition status, and auto upload failure reason are displayed in the Token Details.

Revamping user interface of Device Enrollment Program profile configuration workflow >>

MaaS360 revamps the user interface for Device Enrollment Program (DEP) workflow. The revamp introduces a new tab for configuring Profile and for items that can be skipped for configuration during iOS and macOS DEP device enrollment process. The function of the DEP workflow remains unchanged.

Support to upload shell scripts as an app from MaaS360 Packager >>

Administrators can now use MaaS360 Packager to upload shell scripts to MaaS360 App Catalog as an app. When the app is available in the App Catalog, shell scripts can be distributed just like any other app.

Execution of shell scripts on macOS devices as an action >>

MaaS360 adds support for a new dynamic action for enrolled macOS devices, allowing the administrators to remotely push shell scripts to macOS devices for execution right from the device view. **Note**: The shell scripts are not executed if the device is offline. The shell script execution is only supported on MaaS360 for macOS agent version 2.35.100.003.

Android

Recommendation to adopt Android Enterprise >>

Android in the enterprise is a Google-led initiative that brings together Android and Play to enable users to work the way they want, using the devices and apps they love, while giving IT admins the security and management features they need. Google recommends customers using Android platform to leverage Android Enterprise for their enterprise deployments as opposed to traditional Device Administrator based deployments. MaaS360 is encouraging customers to sign-up for and try Android Enterprise. Signing up for Android Enterprise does not impact existing enrolled devices. Future enrollments have the option to chose between traditional Device Administrator based management and Android Enterprise based management.

Android Enterprise and Samsung Knox harmonization >>

Background: Android Enterprise and Samsung Knox are being harmonized to work together on Samsung devices.

MaaS360 adds support for Samsung Harmonization. With this feature, MaaS360 allows administrators to leverage Samsung Knox APIs for corporate-owned Samsung devices enrolled in DO mode in addition to already supported Android Enterprise API's. In 10.69, MaaS360 adds this capability as new policies for Samsung devices with a new support tag DO with KNOX under Android Enterprise in Android MDM Policy. **Note**: For existing DO enrollments on Samsung devices, users can enable ELM License from Corporate Settings to use this feature. The devices that enroll after 6.25 release are eligible for this feature by default. Supported on Samsung devices running Android OS version 6+.

Enrollment of Work-Managed devices using Samsung KME >>

MaaS360 provides support for KME-based Device Owner mode (Android Enterprise) enrollments. With this feature, organizations can pre-configure work-managed devices through Samsung KME so that devices automatically enroll into MaaS360 in DO mode after the first boot or on device reset. Note: Supports only Device Owner (DO) mode enrollment and applicable only on Samsung devices with Knox 2.8+.

Support to schedule download of Android app updates for corporate apps >>

MaaS360 adds support to schedule download of Android app upgrades for a set time and date to prevent business interruptions. Previously, administrators could only set the upgrade time and date for actual app upgrade installation purpose and not necessarily for the download. In this case, the upgrade date must be greater than upgrade download time. Note: If the download of app upgrade is not scheduled, the download is initiated as soon as the administrator pushes upgrade for the app.

Support for enforcement of device enrollment for DO mode >>

MaaS360 enhances the QR code and Zero Touch enrollment workflows with an option to prevent the users from skipping the device enrollments. In the previous versions, users could skip mandatory screens that were required for enrollments.

Support to easily identify devices that have power saving mode enabled >>

When managed devices enter power saving mode, some features like background data and location services are restricted and MaaS360 agent cannot receive important updates from the MaaS360 portal. To overcome this issue, MaaS360 adds support to identify managed devices that have power saving mode enabled in the device view. Administrators can also use the advanced search to filter all the devices that entered the power saving mode.

Support to schedule device and group-level actions on Zebra and Bluebird devices >>

MaaS360 allows administrators to schedule various actions on Bluebird and Zebra devices to take place during a window of time that does not affect the employee productivity. In this release, MaaS360 adds scheduling support for OS download, upgrade, and copy file actions.

Windows

BETA-User management for Windows 10 Bulk Provisioning Tool >>

MaaS360 extends Windows 10 Bulk Provisioning Tool capabilities for bulk associating users by using device hostname in the bulk upload .csv file.

Export option for Patch Management reports

MaaS360 provides an export option for existing Patch Management workflows so that administrators can download global patch reports. The Patch Management function is accessible from the Security tab in the MaaS360 portal. The workflows OS Patches (Windows), OS Patches (macOS), App Updates (Windows), and App Updates (macOS) supports the export options. The reports are exportable both as a .csv file and excel file. The reports provide overall Patch Compliance status in an environment by listing all patches or app updates that can e missing on any of the devices. The report also provides data about affected devices count against each patch. A list of devices that are missing a specific patch or app update can also be obtained by clicking count of missing devices in the patch management reports.

Support for automatic retry of failed Windows package installations

MaaS360 adds auto-retry support to combat failed Windows packages scheduled for instant installations. With this support, when the instant installation for an app fails, MaaS360 automatically attempts the reinstallation of Windows packages thrice over a period of five minutes until the installation is successful. Note: Supported for .msi, .exe, and scripts type of applications.

Support to define app installation preconditions with relevance criteria >>

MaaS360 allows administrators to define app installation relevance criteria or pre-requisites for Windows enterprise app installations. With this feature, the enterprise apps are installed only on the devices that pass the predefined relevance criteria. This will address scenarios where the app installations failed previously because some of the prerequisites required for successful installation are not met. The apps will be picked up for installation only if install relevance criteria is met.

App Management

App Approval & Publication Process Workflow enhancements >>

MaaS360 adds support to allow the administrators to enable App Approval workflow right from the MaaS360 portal. App Approval & Publication Process Workflow allows administrators to set up quality standards and guidelines for publishing apps to enterprise app store. From the moment a mobile app is conceptualized to the time it is received by an IT administrator and to the time it published to the production users, IT administrators are engaged in a series of processes where they would need to complete the security, compliance and devops processes in order to ensure that the app meets the quality and compliance standards set by the organisation. These steps can be added in a streamlined fashion into the MaaS360 App Approval Workflow. All the applications can be made to pass these requirements before they are being promoted to the App Catalog.

A new role called "App Approver" is also added to primary administrators by default. This role can be assigned to authorized administrators such as Security

officers/compliance officers to grant them privileges to review (accept/reject) apps submitted for approval.

Distribution of Android Enterprise apps for alpha and beta testing >>

MaaS360 adds support for the distribution of pre-release versions of public and private channel Android Enterprise apps for internal testing purposes. The alpha and beta testing tracks allow administrators to receive early feedback from users and fix issues before releasing the app to production.

Email notifications on new permission requests for Android Enterprise apps >>

If automatic re-approval is not enabled for Android Enterprise apps, MaaS360 administrators will receive email notifications when new permissions are requested by that app. Based on this notification, administrators can log in to the MaaS360 portal and easily approve the new permissions right from the MaaS360 App Catalog. The apps that require an administrator to accept new permissions are distinguished with a red exclamation mark over the app icon.

Support to submit macOS apps for approval >>

MaaS360 extends app approval workflow support to macOS apps. With this support, administrators can submit iTunes and enterprise apps for app approval before promoting those apps to App Catalog. Previously, the App Approval workflow was limited to Android, Windows, and iOS apps.

Installation of enterprise apps on App Catalog agent with support to view installation progress >>

MaaS360 enhances macOS App Catalog agent to handle installations of custom enterprise apps with the support to view installation status on a progress bar. Previously, the enterprise apps were installed via MDM.

Cloud Extender

Delete users without active Cloud Extender devices >>

Maas360 enables admins to delete users without any active Cloud Extender devices

New Configuration Tool UI >>

MaaS360 Cloud Extender design teams have begun implementing changes to the CE interface based on client feedback. That new UI is now ready for clients, and is available to all of you! The core functionality remains the same, but this UI streamlines the setup, maintenance, and backup/restore processes.

Platform

Permanently delete Apple School Manager user accounts in MaaS360 portal >>

MaaS360 supports automated method of permanent deletion of Apple School Manager (ASM) users and extends support for deletion of Local Education users both manually from the MaaS360 portal and also automated method. The automated method refers to deactivating the ASM user account from ASM portal. The ASM user account is automatically removed from the MaaS360 portal based on the duration set for permanent deletion.

Engage Professional Services >>

Maas360 adds Engage Professional Services link to the existing Help menu.

Track the re-activation or re-registration time of a device >>

Maas360 introduces an attribute to capture the last activation time for a device enabling admin to capture time of registration for re-enrolled devices.

Customers and Partners

Add or update Primary Administrator for a MaaS360 customer and partner account >>

MaaS360 allows Administrators with relevant permissions to mark an administrator as a Primary Administrator for a customer and partner account.

New and improved UI for Maas360 customer and partner administrators >>

The revamped UI will be official for all customer and partner administrators upon login.

Analytics

Business Dashboards for Apps >>

MaaS360 extends the availability of Business Dashboards for Apps (Apps Inventory) to new and existing customers. The reporting data provides overview and trends statistics in Business Dashboards for Apps for managed and non-managed apps. The dashboards provide an overview for all apps along with usage, execution trends & statistics for enterprise apps which have MaaS360 SDK in them. Contact IBM MaaS360 Customer Support Team to avail Business Dashboards for Apps. Customers must be on the new MaaS360 portal user interface to view Business Dashboards for Apps.

Business Dashboards for Apps availability for SPS only mode MaaS360 customers

MaaS360 extends Business Dashboards for Apps (Apps Inventory) availability for SPS only mode customers. The Business Dashboards for Apps are accessible from Reports menu in the MaaS360 portal for all enterprise apps with MaaS360 SDK in them. Contact IBM MaaS360 Customer Support Team to avail Business Dashboards for Apps. On accessing Business Dashboards for Apps, SPS mode customers can view Usage Overview, Execution Overview, usage Trends, and Execution Trends reports.

General availability of Business Template Based Policy and Community Based Policy to all MaaS360 customers >>

MaaS360 introduces Business Template Based policy and Community Based policy to all customers. The function enables customers to add policy based on business use case needs and community insights.

Azure Active Directory integration

Beta feature: Azure Active Directory device status update >>

MaaS360 introduces a new customer property called Azure AD Device Status Updates. This feature allows administrators to synchronize compliance status in MaaS360 with the Azure Device Directory for Windows 10 devices that are enrolled through the Windows OOBE enrollment mode. You must contact IBM Support to enable this feature for your account.

Azure AD and On-Premises AD mixed-mode support >>

MaaS360 introduces support for Azure Authentication and AD/LDAP Authentication mixed-mode setup.

10.68 Release Summary

iOS / macOS MDM

Configure Apps Purchase Program from Settings page >>

MaaS360 includes Apps Purchase Program settings under App Settings in the Settings page to allow administrators to easily access and configure all required settings including Volume Purchase Program (VPP) from this page.

Auto upload Apple VPP applications to the MaaS360 portal by using VPP token >>

MaaS360 introduces capabilities to automatically upload all Volume Purchase Program (VPP) applications associated with a VPP token to MaaS360 App Catalog in the portal. Previously, applications associated with a VPP token had to be manually uploaded to the MaaS360 App Catalog in application portal.

New Classroom Restrictions supported in iOS Supervised Settings >>

MaaS360 introduces Classroom Restrictions to manage Apple Classroom. Join Classes Automatically, Request Permission to Leave Classes, Allow App and Device Lock without Prompt, and Allow Screen Observation without Prompt Classroom Restrictions are introduced. You can enable these restrictions from iOS MDM policy > Supervised Settings > Restrictions & Network > Classroom Restrictions.

Handle inactive devices mapped as User Removed Control from Apple Feedback Service >>

MaaS360 introduces a mechanism to recover inactive devices that are marked as User Removed Control by Apple Feedback Service. New methods to handle inputs from Apple Feedback Service is introduced in this release wherein devices that are not available to receive the push notification from Apple or MaaS360 are marked as Unreachable. Previously, such devices were marked as User Removed Control.

New settings in macOS Wi-Fi configuration >>

MaaS360 introduces additional Wi-Fi settings such as Disable Captive Network Detection and Enable QoS Marking for Apps in macOS MDM policy. You can configure these settings from macOS MDM policy > Configuration > Wi-Fi.

Option to skip setup of parameters during DEP Profile configuration >>

MaaS360 includes FileVault, iCloud Diagnostics, iCloud Storage, and Registration parameters under 'Skip Setup Items' in DEP Profile configuration. Customers can enable these parameters in DEP profile configuration and choose to skip configuration of these settings during macOS DEP device enrollment process.

New restrictions added in macOS Passcode settings >>

MaaS360 introduces additional passcode restrictions in macOS MDM policy such as Grace Period for Device Unlock without Passcode in Minutes, Number of Unique Passcodes Required Before Reuse Allowed (1-50, or blank), and Reset Passcode on Next Authentication. You can enable these settings from macOS MDM policy > Restrictions > Password.

New restrictions added in macOS Device Functionality Restrictions >>

MaaS360 introduces additional device functionality restrictions in macOS MDM policy. You can enable these settings from macOS MDM policy > Restrictions > Functionality. The restrictions are supported on macOS 10.12+ devices only. Allow use of Camera and Configure Delay for Software Updates are supported on macOS 10.11+ and macOS 10.13+ devices respectively.

Encrypt all outgoing messages >>

MaaS360 adds support for S/MIME on Exchange ActiveSync with options to individually enable or disable signing and encryption on all outgoing messages by default. In the previous releases, all the messages were automatically encrypted and signed on pushing down the signing and encryption certificates to the devices.

CalDAV enhancements >>

MaaS360 allows the administrators to set up CalDAV to sync enterprise calendar so that all the users access the same calendar on macOS devices. Previously, macOS users could only sync personal calendars using the corporate username and password.

Support for Provider Type for Pulse Secure VPN profile >>

MaaS360 allows administrators to deploy Provider Type value in the Pulse Secure VPN profile. With this support, administrators can tunnel the VPN traffic either at the application layer or at IP layer.

Android

Support for secure TeamViewer unattended access (beta) >>

MaaS360 adds support for secure TeamViewer unattended access, allowing the administrators to set up permanent access to remote devices by using the

TeamViewer Host app for Android. With this support, administrators can silently install the host app on the remote devices and initiate unattended remote support without any action to be taken on the remote side. In the previous releases, MaaS360 added support for TeamViewer attended access.

The list of supported devices is provided here.

Support for disabling of passcode on MaaS360 agents through Android Configurator >>

Background: MaaS360 users can use passcode settings in the MaaS360 agent to lock the MaaS360 application, even though the passcode is not enforced through Secure Policies.

In 10.68, MaaS360 enhances the bulk enrollment feature to allow the administrators to disable the passcode settings on the device. As a result, the passcode settings are unavailable in the MaaS360 agent after the enrollment.

Support for disabling device reset on failed passcode attempts

Background: Administrators can use Maximum Failed Passcode Attempts policy to specify the number of times a user can enter an incorrect passcode before the device is completely wiped. In Android Enterprise devices, the Android Enterprise profile is erased on maximum failed passcode attempts.

In this release, MaaS360 now allows administrators to specify 0-16 values in the Maximum Failed Passcode Attempts field as opposed to previously allowed 4-16 values. The value 0 (zero) indicates that the policy is disabled, and the devices are not wiped on any number of failed passcode attempts.

OEMs

Build number validation before performing OS upgrade on Bluebird and Zebra devices >>

MaaS360 now validates the target build number against the current build number before performing an OS upgrade on the Bluebird devices. With this enhancement, the download is initiated only if the target build number is different from the build number already available on the device. Previously, the validation was performed after the OS update zip files were downloaded.

Support for new group-level action to copy files from a remote server >>

MaaS360 adds a new group-level dynamic action to allow the administrators to easily copy a file to a group of Zebra and Bluebird devices from a remote server.

Support for new push profile actions on Bluebird devices >>

MaaS360 adds support for real-time actions, allowing the administrators to deploy predefined profiles that take specific action on the managed Bluebird devices.

M3 Device Management >>

MaaS360 announces a partnership with M3 to manage ruggedized SM10 devices in the MaaS360 platform. This release marks the first phase of a series of enhancements to be made to the MaaS360 platform to integrate with M3 SM10 devices. MaaS360 adds support for silent installation/upgrade of apps and new policies to enforce device restrictions on M3 devices. Requires Android 6.20+ agent. **Note**: MaaS360 only supports SM10 devices in this release.

Windows

BETA Windows 10 Bulk Provisioning Tool >>

MaaS360 introduces Windows 10 Bulk Provisioning Tool that allows administrators to automatically enroll Windows 10 Laptops when using standard imaging process followed in their organization.

Use Patch Source Category for effective Patch Distribution >>

In order to power administrators to make decisions on what patches need to be distributed to Windows and Mac devices, patch category is displayed as Source Category. For each patch, Source Category is now displayed which identifies the category of the patch. Patches can be filtered based upon the type of Source Category. Multi-select filter option is also supported for the category selection so that a bunch of patches of a certain category can be distributed to devices. This capability is available for both type of patches - OS Patches and App Updates on Windows and Mac devices.

Windows Phone App Updates

MaaS360 announces updates for Windows Phone Email, MaaS360 Docs, and MaaS360 Browser. A new version 2.8.1 is now available in Windows Marketplace that contains minor bug fixes.

Support for new real-time actions for Windows devices on MaaS360 End User Portal (EUP) >>

MaaS360 adds support for new real-time dynamic actions in MaaS360 End User Portal (EUP), allowing the end-users to easily perform actions such as lock device, wipe, locate, remove control, etc., on Windows 10 enrolled devices. Previously, EUP supported these actions for Android and iOS platforms.

Support for viewing app installation status and canceling app installation in Windows App Catalog >>

MaaS360 allows users to view all the stages of the app installation on Windows App Catalog. MaaS360 also provides an option to cancel the installation, just in case end-users no longer want to download the app.

Support to enable debug logging for MaaS360 Windows agents >>

MaaS360 adds debug logging support, allowing the administrators to produce a detailed log of application activity captured from supported Windows agents. The diagnostic logs help the support team to troubleshoot issues by pinpointing the cause of the problem. Previously, the options to enable debug logs and upload logs were restricted to MaaS360 support team.

MaaS360 Platform

General availability of Unified Enrollment >>

MaaS360 announces the general availability of Unified Enrollment for all new and existing MaaS360 customers.

Support for filter option for all columns in Policies user interface >>

MaaS360 enhances Policies usability for customers by introducing filter options across all columns in the Policies page. The filter option enables customers to easily search the required policies based upon various search criteria that is supported for all columns in the Policies page.

Availability of new user interface for application portal for all MaaS360 customers and partners >>

MaaS360 offers an improved user interface (UI) for administrators. The new UI that was released a few months back is now enhanced to show more content on the UI pages and offers a consistent experience across the MaaS360 portal.

Support to register a device without requiring a Flash player >>

MaaS360 removes the dependency on Flash player to register a device. With this feature, if strong authentication is enforced, administrators can seamlessly register a device and avoid security checks to access the MaaS360 portal. However, with 10.68, the administrators that already registered their devices will need to go through the additional security check once again to re-register their devices. Previously, when the Flash is blocked, administrators had to go through security checks even though the devices were successfully registered.

Swedish language support >>

MaaS360 adds Swedish language support across the MaaS360 portal, End User Portal, and MaaS360 agents.

Support for time-based two-factor authentication for FedRAMP compliance >>

MaaS360 reinforces security by adding a time-based two-factor authentication support for portal administrators to meet the requirements of US Federal Risk and Authorization Management Program (FedRAMP). With this support, administrators must use a time-based one-time passcode in addition to their login credentials for authentication. In the previous releases, MaaS360 supported OTP via email and SMS.

Device group evaluation mode label change >>

The **Real-time** field in Evaluation Mode column that is used to filter the device groups based on device group evaluation has been renamed to **Batch and Enrollment**.

Misc

Various bug and security fixes. Thanks to Cody Wass of NetSPI for responsible disclosure of an XXE issue.

Analytics

Enhancements in Software Overview reports >>

MaaS360 includes additional customization columns such as Platform Serial Number and Device Serial Number in the App Inventory reports also known as Software Overview reports.

Apps

Support to add the same app from different sources in MaaS360 App Catalog >>

MaaS360 adds support to upload the same app from different sources in MaaS360 App Catalog. For example, if an app is uploaded as a Google Play Store, the same app (with the same bundle ID and version) can be uploaded as an Enterprise app from MaaS360 App Catalog. With this feature, customers that do not have access to Google Play Store can upload apps through other channels without conflicting the apps already available in MaaS360 App Catalog. **Note**: Contact MaaS360 support team to enable this feature for your account.

Cloud Extender 2.94

Enhancements to certificate updates in the MaaS360 Portal (Update Device Certificate) action >>

MaaS360 now allows administrators to update a single certificate or multiple certificates on devices that are enrolled in the MaaS360 Portal that use the MDM policy and the Persona policy.

10.67 Release Summary

iOS / macOS MDM

iOS 11.3 enhancements >>

MaaS360 announces following iOS 11.3 enhancements:

>> Enable authentication for autofill

This restriction enforces Face ID authentication on iOS 11.0+ devices before autofill of password or credit card information action happens in Safari browser or Apps. This function is supported on iOS devices with face identification support.

>> Configure delay for software updates

This restriction forcefully delays device software updates on iOS 11.3+ devices for the number of days the restriction is applied. User visibility to software updates is restricted.

>> Option to skip privacy screen setup during the addition of DEP profile

The following screen setup can be skipped during iOS 11.3+ DEP device enrollment. Home Button Sensitivity, Privacy, OnBoarding, Touch ID settings, and ToC is renamed as Terms and Conditions are included in **Skip Setup Items** list during the addition of new DEP profile.

>> Option to skip proximity setup during device wipe action

MaaS360 provides **Disable Proximity Setup on next reboot** setting in device wipe action. This setting disables support for automatic setup on iOS 11.3+ devices. Automatic setup is Apple feature that helps set up your new iPhone 8 / iPhone 8 Plus / iPhone X, by just holding your new Apple device near an iOS 11.0+ device you already own.

Delete Apple School Manager (ASM) data from MaaS360 portal >>

MaaS360 introduces support to delete synced Apple School Manager (ASM) data from MaaS360 application portal. Contact IBM MaaS360 Customer Support team to request deletion of synced ASM data from the portal. On completion of ASM data deletion, ASM integration with MaaS360 is disabled by default and if needed, customer administrator might manually enable ASM integration from the MaaS360 portal.

Auto naming for DEP devices displays detailed model name >>

MaaS360 extends capabilities to display detailed model name for auto naming enabled DEP enrolled ioS devices. Previously, the model name displayed device model such as iPhone, iPad, iPadAir. From this release, the model name includes specific details of device model such as iPad 7, iPhone 6 Plus., hence allowing display of more meaningful model names.

Device custom attributes support for iOS policy settings >>

MaaS360 extends support for including device custom attributes as placeholder values in iPCU settings and anywhere with %attribute_name% in iOS policy.

Configure cellular roaming settings by using Web Services API

MaaS360 introduces Web Services API function to configure cellular roaming settings for an iOS device. This function is in addition to the existing iOS policy settings for configuring cellular roaming profile from **Advanced Settings** > **Cellular** in an iOS policy. Customers can invoke APIs that are specific to cellular roaming settings and configure data roaming and voice call roaming settings for an iOS device. MaaS360 support for configuring cellular roaming settings by using iOS policy remains unaffected by this functionality.

AirPrint printer configuration for macOS >>

MaaS360 extends configuration of AirPrint printers from iOS to macOS MDM devices. New attribute that is called **AirPrint** is added under **Configuration** setting in macOS MDM policy. The function allows devices that are connected to the same network to print over the air via Wi-Fi.

Swedish language support on macOS agents

MaaS360 adds Swedish language support for MaaS360 App Catalog, Packager, and macOS agent.

Static password support for macOS WPA/WPA2 (Enterprise) Wi-Fi profile

MaaS360 extends static password support for macOS WPA/WPA2 (Enterprise) profiles. In the previous releases, the support was only available for

iOS policies. With this support, when the policy reaches the device, macOS devices automatically gain access to corporate Wi-Fi network without authentication.

New restrictions added in macOS System Preferences

MaaS360 adds two new restrictions such as **TouchID** and **Wallet & Apple Pay** settings. You can enable these settings from macOS MDM policy > Restrictions > System Preferences.

New alerts for VPP and DEP in MaaS360 My Alert Center

MaaS360 adds new alerts for VPP and DEP services to notify customers about VPP or DEP client context mismatch and DEP T&C validity expiry. These alerts are displayed in **My Alert Center** in the MaaS360 portal home page. The alerts are included in addition to the existing VPP and DEP alerts for token expiry.

Locked profiles for iOS support is disabled in MaaS360 instance

MaaS360 announces the end of life for MaaS360 Security Profile (Locked Profile) for iOS support in MaaS360 M1 instance. This support withdrawal impacts only for those customers with Locked Profile for iOS support enabled for their MaaS360 accounts. During enrollment, an additional profile was being pushed along with MDM profile if Lock Profile for iOS support was enabled for the customer account. With disablement of Locked Profile support from 10.67 release, this function is no more allowed for a customer account. Note: For those profiles that are added until this release, it remains unaffected by this function disablement.

Android

Support for Chrome OS (Chromebook) device management >>

MaaS360 announces a partnership with Google to manage Chrome OS devices alongside other endpoints in an enterprise from a single unified management solution. With this support, administrators can easily enroll Chromebooks into MaaS360 portal via Google admin console. MaaS360 also leverages Google APIs to allow the administrators to enforce security policies on Chome OS devices.

Note: This feature is beta at this moment. Please contact MaaS360 support in order to enable this feature.

Trusteer Threat Management enhancements >>

MaaS360 adds support for enforcing the Trusteer Threat Management policies through Persona policies for mixed mode (MDM+SPS) customers.

Dual SIM card reporting >>

If a dual-SIM card device is enrolled, the MaaS360 agent now reports network information pertaining to both the SIMs to MaaS360 portal. With this support, MaaS360 also allows the administrators to search a device by its secondary SIM ICCID and IMEI numbers.

Support for auto-renewal of certificates for secondary accounts

MaaS360 adds support for automatic certificate request and renewal support for secondary accounts. With this support, the MaaS360 agent automatically sends a certificate request and renews the certificates in the background. Previously, the secondary accounts had to be re-configured on certificate expiration.

Platform

Web Services API for Device Group refresh action >>

MaaS360 introduces API for Device Group refresh action in addition to the existing Refresh action in the MaaS360 portal user interface (UI). The API when invoked, performs the same action as existing refresh action on the UI. From this release, a total number of 500 refresh attempts are allowed for a customer account for a day (based on UTC time format). This limit count of 500 is inclusive of both API and UI refresh actions.

Auto-provisioning enhancements for portal administrators account- phase II >>

MaaS360 enhances sync process between the corporate directory and MaaS360 portal for auto-provisioned administrator accounts. The enhancement includes an asynchronous method of fetching portal administrator account status from Active Directory (AD) by using Cloud Extender 2.94 module. This module offers periodic checks and deactivates any auto-provisioned account if the user account is no longer in AD or not included in an auto-provisioned group.

Search by Platform Serial Number in Global Search >>

MaaS360 adds support to search devices by Platform Serial Number device attribute in Global Search in addition to other search parameters that Global Search currently supports. Search by Platform Serial Number is supported only for Android and iOS device platforms.

End User Portal (EUP) enhancements >>

MaaS360 provides resolution for End User Portal (EUP) error that occurs when a user tries to reset new login password by using 'Forgot Password' link. Previously, users had to contact an administrator to reset the password. The fix that is provided in this release is applicable only for user accounts with auto-generate user password settings.

Revamped user experience when inviting additional administrators >>

MaaS360 introduces an upgrade to invite user forms based on new user experience design. These forms are replacing the existing forms that are used by a new portal administrator to signup to an IBMid for getting access to a MaaS360 subscription. In this scenario, if a new administrator does not previously have an IBMid, the administrator receives an invite email with a URL. This URL can be used for signing up to an IBMid before accessing MaaS360 account.

Enhancements to retrieve MaaS360 login credentials >>

MaaS360 enhances username and password retrieval method for portal login. If customers forgot MaaS360 login credentials, it can be retrieved by using the instructions sent to their registered email address. This function is supported only for customer accounts that use MaaS360 credentials for authentication mode. This function is not supported for AD, LDAP, SAML, and IBMid authentication methods. Previously, only password retrieval was supported and to retrieve username, customers had to contact IBM MaaS360 Customer Support team.

MaaS360 also launches a single URL login.maas360.com that customers can use to login to MaaS360 account irrespective of MaaS360 instance in which the customers hold an account.

Single page for configuring MaaS360 Settings >>

MaaS360 introduces a single Settings page that allows customers and partners to easily access MaaS360 settings from one location under **Settings** page. The following settings are accessible from Settings page for customers: Device enrollment settings, User settings, App Settings, Doc settings, and Administrator settings. Partners can manage these settings for customers accounts under them. To avail this capability, MaaS360 customers and partners need to be on the new user interface.

Partners

MaaS360 partners get new user interface for application portal >>

MaaS360 extends new user interface (UI) for application portal to partners. In the previous release, this feature was limited to customer accounts. All new MaaS360 partners get new UI by default. Existing MaaS360 partner accounts that are created post 10.66 release gets old UI by default with an option to toggle between old and new UI from the portal. New customer accounts created post 10.66 under any partner account, continue to remain on new UI with no toggle option and pre 10.66 customers continue to get toggle option between new and old UI.

Windows

Support for Microsoft HoloLens device management >>

MaaS360 announces a partnership with Windows to manage HoloLens devices alongside other endpoints in an enterprise from a single unified management solution. With this support, administrators can easily enroll Windows HoloLens devices into MaaS360 using the normal enrollment workflow. MaaS360 also leverages Windows APIs to allow the administrators to enforce security policies, compliance riles, and device actions on HoloLens devices.

Support for new device-level action on Windows 10 devices >>

MaaS360 adds new device-level action to allow the administrators to upgrade licenses and change product key on Windows 10 devices.

Cloud Extender and MEG 2.94

Support for multiple Cloud Extender masters in an Exchange environment (both On-Premises Exchange 2010, 2013, 2016 servers and Office 365 servers) >>

The Cloud Extender 2.94 release removes the functionality that only allowed the administrator to designate one master Cloud Extender in an Exchange environment. Multiple Cloud Extenders now collaborate through a shared data area to determine which Cloud Extender becomes the master. This new functionality eliminates any issues that an administrator might encounter with misconfiguring a designated master Cloud Extender, since configuration is done in the background.

MEG syslog integration with IBM Security QRadar >>

IBM Security QRadar can now collect MEG gateway authentication and resource logs via any configured syslog server.

10.66 Release Notes

iOS / macOS MDM

Enroll Non-DEP iOS 11 devices from Apple Configurator using enrollment URL >>

Apple allows MDM Enrollment of a non-DEP device via Apple Configurator by providing an MDM server URL. To support this feature, in the 10.66 platform release the MaaS360 portal will provide 2 URLs, one that prompts for authentication and the other that does not require authentication. The enrolling devices are not converted to a DEP device.

DNS proxy support within MDM Policy for iOS 11.0+ devices >>

This release provides a new MDM policy under the Advanced settings that allows the Administrator to enter DNS proxy payloads for all iOS 11.0+ devices. The DNS proxy includes configuration options for the Apple Bundle ID, Provider Bundle ID, and Provider Configuration.

Preserve data plan attribute for iOS 11.0+ devices >>

MaaS360 builds capabilities in the application portal that support the Preserve Data Plan attribute introduced by Apple for Mobile Device Management. Only for iOS 11.0+ devices, during the process of wiping or erasing a device, the Administrator can now enable the Preserve Data Plan option in the Portal to preserve an active data plan consumption value on the device that is being wiped or erased.

Update device certificate for iOS devices configured with Persona policy >>

MaaS360 extends an option to update the device certificate for iOS activated and enrolled devices with the Persona policy. This feature is the same option as updating certificates for MDM enrolled iOS devices.

Windows

L2TP VPN Support for Windows 10+MDM Laptop and Desktop devices >>

MaaS360 adds support for yet another type of VPN connection for Windows 10+ MDM Laptop and Desktop devices - L2TP/IPSec VPN. The L2TP VPN configuration currently supports only password based authentication for users and works based on pre-shared key (PSK).

Windows App Catalog enhancements >>

MaaS360 adds a lot of great features in Windows App Catalog (portal) including: **distribution of scripts**, with support for installation context and execution commands; **distribution of documents**, with support for downloading documents to specified location; **distribution of web apps**, with support for opening web apps using MaaS360 Secure Browser; **distribution of app bundles**, with support for adding app bundles to featured apps section. Additionally, MaaS360 adds an option to mark an app as a featured app so that the app is displayed in the Featured section in the App Catalog agent.

Windows App Catalog agent enhancements >>

MaaS360 introduces featured apps carousel, redesigned user interface, and default filters to sort apps. Also, MaaS360 adds support for viewing installation count, providing app reviews and ratings and more.

Android

Support for new group level actions for Zebra and Bluebird devices >>

MaaS360 adds new real-time dynamic actions, allowing administrators to easily perform actions such as OS upgrades, downgrades, and security patch installation on Zebra and Bluebird devices.

Support for Complex Numeric passcode restriction >>

MaaS360 adds support for complex numeric passcode restriction in Secure policies to allow the administrators to enforce a passcode containing numeric characters without repeating or consecutive numbers like 1111 or 1234. This feature is available in both Android MDM and Android Enterprise policies.

EFOTA: Support for publishing dummy firmware on test devices >>

MaaS360 adds support for rolling out a dummy firmware update, allowing the administrators to simulate that update on test device(s) before pushing

to all the devices. Previously, the administrators had to create a separate group for testing purposes.

Android Enterprise

Advanced Android Zero-Touch enrollment support for Android Enterprise devices >>

MaaS360 announces support for Advanced Android Zero-Touch enrollment, allowing administrators to pre-configure devices before the devices are shipped to users. With this feature, corporate-owned devices can be deployed in bulk without having to manually set up each device.

Support for enrollment through QR Code on Android Enterprise devices >>

MaaS360 simplifies the enrollment process by allowing the administrators to deploy enrollment settings during the QR code enrollment. Previously, only Wi-Fi settings were deployed through QR code based enrollment. This feature eliminates the need to create a separate enrollment request for Android Enterprise devices.

Platform

Departmentalization based on Device Groups >>

MaaS360 extends Departmentalization to Device Groups, similar to existing User Group based departmentalization. This feature allows Device Group Administrators to manage Device Groups and perform app distribution, policy and rule-set assignments on devices.

Auto-provisioning enhancements for portal administrator accounts >>

MaaS360 enhances auto-provisioning administrator accounts by syncing administrator account login between the corporate directory and the MaaS360 Portal. With this enhancement, auto-provisioned administrator accounts that are disabled or deleted cannot log in to MaaS360 Portal. Also, any administrator account that is no longer part of an auto-provisioned group cannot log in to MaaS360 Portal.

New user interface for MaaS360 application portal >>

MaaS360 introduces a new user interface (UI) for the MaaS360 Portal. For 10.66 and later releases, the new UI for the MaaS360 Portal is made available by default to all new customers. Existing MaaS360 customers are provided an option in the Portal under the User Profile to switch between the new and the existing UI.

- **UI revamp in MaaS360 portal for Portal Administration >>**

MaaS360 enhances the Portal Administration page by revamping the user interface with a new UI design. UI elements such as Grid with filters to display administrator details, Column Customization, Reset Filters, and CSV to export administrator details are added.

- **UI revamp in MaaS360 portal for Administrator Logins Report >>**

MaaS360 enhances the Administrator Logins Report page by revamping the user interface with a new UI design. UI elements such as Grid with filters to display administrator login report details, Reset Filters, and CSV to export administrator login reports are added.

New Quick Start wizard with new MaaS360 user interface >>

MaaS360 redesigns the existing Quick Start wizard. The new wizard is designed to offer administrators essential information that is required at each step during the Quick Start configuration. Additionally, Security Policy and Configuring native email settings are added in the new Quick Start wizard to help administrators configure the necessary settings that are required to get started with MaaS360. More enhancements are coming in future releases that offer a seamless MaaS360 deployment experience. From this release, the new Quick Start is available by default for all new customers. Existing MaaS360 customers can access the new Quick Start by using the 'Switch to new UI' option available under the User Profile.

Support for App Approval Workflow >>

MaaS360 adds support for app approval workflow to allow administrators to set up quality standards and guidelines for the app store. An application that is submitted to the app store must pass those requirements before it is published. In the first phase of series of enhancements, MaaS360 primarily focussed on roles and privileges that are required for managing app approvals.

Cloud Extender

Simultaneously refresh device certificates on multiple devices >>

This release of Cloud Extender enhances the workflow for refreshing all certificates on a device. In previous releases (10.65 and earlier), the administrator accessed the Device Details page and manually selected a device to refresh that certificate. With this release, the administrator can now use the Update Certificate option on the Device Inventory page to refresh certificates on multiple devices all at once.

New setting for AD Account Lockout on Deployment Settings page >>

This release enhances Active Directory account lockout options from previous releases (10.65 and earlier) by providing a new account lockout setting on the Cloud Extender Deployment Settings page in the MaaS360 Portal. Administrators can now configure how many times a user provides a password to access the corporate directory for Active Directory authentication before the account is locked for a specific period of time (in hours). This feature prevents users from being locked out of their account indefinitely, which then requires an administrator to manually reset the user account password.

Multiple Secure Mail notifications support for Cloud Extender mail accounts on iOS devices >>

MaaS360 extends support for multiple Secure Mail accounts that was introduced in the 10.65 release. This feature allows administrators to configure and enable email notification settings for both primary and secondary Secure Mail accounts configured on an iOS device.

Partner only information

Inherit end-user notification settings and app distribution settings from Partner account >>

MaaS360 introduces capabilities to inherit settings such as End User Notifications and App Distribution settings from parent Partner account to all customer and partner accounts that are created under parent Partner account.

10.65 Release Notes

iOS / macOS MDM

Support for adding any iOS 11 device to DEP >>

With iOS 11, Apple introduced the ability to add any iOS device to a DEP account. The iOS device need not have been procured through the traditional DEP channel. MaaS360 introduces new capabilities to support this new iOS 11 functionality. Administrators now have the capability to add such devices to their DEP account using MaaS360 workflows. MaaS360 supports authenticated and unauthenticated enrollment of devices into MaaS360 while still requiring DEP authentication for new device additions. Users have the ability to leave DEP management for a period of 30 days post addition after which the device will be permanently associated with the corporate DEP account.

Support for Unified Enrollment for macOS >>

macOS devices enrollments now support the new MaaS360 Unified Enrollment experience. Previously, macOS enrollments started with users downloading the MaaS360 agent on the device. With this change, customers currently using the new Unified Enrollment workflows on iOS and Android will now see a new experience on macOS devices. Users will start the enrollment from a Safari browser and complete the enrollment process. MaaS360 agent will get installed post enrollment, just like iOS. With the unified enrollment support on macOS, customers can leverage other features like Enroll on behalf of, the new two-factor authentication based enrollment and SAML authentication for macOS devices. Customer that are not leveraging the Unified Enrollment experience will see no changes in the enrollment experience on macOS.

De-couple application whitelist and VPN configuration for per-app VPN configuration >>

In this release, MaaS360 has de-coupled the configuration of VPN and the application whitelist for per-app VPN configuration. Previously, if a new app needed to be added to the application whitelist for participation in per-app VPN, the entire VPN configuration would be re-loaded on the iOS device. This would also include re-issuing a certificate to the device. With this release, administrators can now add new apps to the app whitelist without re-issuing certificates or reloading their VPN configurations. This will result in faster policy changes and no impact to the end user and enterprise PKI infrastructure.

Support for OS Patch Compliance for macOS devices >>

With this release, administrators can now enforce automated actions on macOS devices missing critical, important and moderate patches. macOS devices that enroll into MaaS360 start reporting the patches that are missing based on severity. Administrators can now define a compliance rule that can enforce actions like alert, corporate wipe, change policy, remove MDM control or factory reset on devices missing a defined number of patches per severity. This feature is also supported on Windows devices.

Support for world's first official iOS screen sharing solution with MaaS360/TeamViewer integration >>

MaaS360 announces support for TeamViewer integration for iOS 11 and later, allowing the administrators to see a user's device in real-time for remote support. With this feature, administrators can kick off sessions via MaaS360 workflows and speed up the troubleshooting process.

Windows

Support for new quick start actions for Windows laptops and desktops >>

As part of the MaaS360 Quick Start workflow that shows up on initial account sign-up, MaaS360 adds three new quick start actions: **Lock**, **Send Message**, and **Locate** for Windows laptops enrolled through DTM. Previously, the quick start actions were only supported for Windows devices enrolled through MDM.

Custom OMA (Open Mobile Alliance) support to deploy configuration settings on Windows devices >>

MaaS360 introduces a way for administrators to push custom policies in the form of OMA configuration files to Windows devices. When Microsoft releases new APIs as a part of their OS release, customers can use this new workflow to push custom policy settings without having to wait for MaaS360 policies UI to be updated. Contact MaaS360 customer support team to enable this feature for your account.

Localization support and redesigned user interface for Windows App Management Utility >>

MaaS360 adds localization support for Windows App Management Admin Utility app to make the app available in 14 new languages. The app also gets a rich and reorganized user interface.

Support for new MaaS360 DTM v3.93 installer >>

MaaS360 introduces DTM installer version 3.93 with updated code base for seamless enrollments. MaaS360 automatically uninstalls BigFix agent on removing device control and is the agent which supports TLS 1.0 deprecation.

UEM Windows/macOS

Support for role-specific access rights for patch distribution >>

In this release, MaaS360 introduces four new access rights for administrators to view/enable patch distribution capabilities at organization level or device level. With this approach, the patch distribution access rights can be restricted to authorized users. Existing administrators with appropriate levels of access will continue to be able to distribute patches. Administrators can then assign this new access right to newly created administrators and also include them as a part of custom role definitions.

Legacy BigFix menus hidden on enabling UEM or BFLTM and other UI changes >>

MaaS360 hides menu items pertaining to legacy BigFix patch management when the latest UEM services are enabled. With the new UEM service for laptops and desktops, administrators can access real-time patch management reports and distribute patches from these screens thereby not requiring the legacy reports. In this release, the laptop and desktop management service options in Setup menu are reorganized.

New system restart delay options for patch download >>

Previously, MaaS360 patching for Windows or Mac allowed for a delay in a restart for up to 1 day after a patch is applied. The system restart delay options are enhanced to support more granular frequencies from 1 minute to 30 days.

Platform

New navigation bar in MaaS360 portal >>

MaaS360 introduces a new navigation bar to the MaaS360 portal in this release. The navigation bar has been redesigned to accommodate new menu items and the options have been reorganized for ease of access. This is a part of the enhancements around usability and user experience that will be introduced in MaaS360 in multiple upcoming releases.

Enhancements to reset MaaS360 portal login password >>

MaaS360 enhances the password reset workflow for administrators logging in to the MaaS360 portal. With changes to the workflow, administrators can unlock their locked accounts with the **Forgot your password** link. The administrators will receive an email to a link to set a new password. This will also unlock the account, which previously required a call to MaaS360 Customer Support.

SAML authentication and portal session passcode for MaaS360 actions >>

With SAML based authentication for MaaS360 portal administration, administrators had to previously enter a unique one-time passcode to approve any action during their logon session. This passcode used to be unique per action and then would be emailed to the administrator each time. In this release, MaaS360 enhances usability to customer administrators logging into the portal via SAML authentication by introducing a **Portal Session Passcode** for actions. The administrator receives one passcode for an active logon session and this Portal Session Passcode can be used to authenticate all actions in MaaS360.

Display supporting platforms and version labels for Compliance Rules >>

MaaS360 has enhanced its compliance rule engine to add support for various device platforms and new compliance rules being supported. In this release, each compliance rule uses labels to identify the supported platforms (iOS, Android, Windows, and macOS). Hovering over the labels displays specific version requirements for these rules.

Support for renaming portal administration roles >>

MaaS360 now allows administrators to edit **Role Name** when editing an existing role. Previously for existing roles, only the Role Description and Grant Access Rights were editable. With this change, administrators can easily edit names without having to recreate a role with a new name.

Support pages help links in MaaS360 portal >>

MaaS360 portal now contains links to the IBM MaaS360 Knowledge Center, IBM developerWorks, and other IBM support pages for quick and easy access to relevant documentation. The portal Help icon also points to helpful links for documentation about MaaS360 product and usage.

Android

Support for location based policies for offline devices and more >>

MaaS360 extends the location based policy support to offline devices. When the device is online, MaaS360 agent automatically downloads all the policies and locations that are assigned to the device. When the device checks into the defined location, an appropriate policy is applied even though the device is offline. Also, MaaS360 adds a new policy to configure Wi-Fi proxy on Samsung devices.

Support for restricting logon hours to company working hours >>

MaaS360 adds logon hours support to make it easier for administrators to configure the days and hours when users can access the email server.

When the logon hours expire, MaaS360 automatically stops syncing from the email servers.

Enhancements to Trusteer Threat Management >>

MaaS360 enhances Trusteer Threat Management with new features to detect Wi-Fi security level, root hider software installed on devices, and whitelisted app details.

Android Enterprise

Support for new Android Enterprise policies >>

MaaS360 adds new policies for Bluetooth sharing, factory reset protection, and allowed idle time for stronger authentication.

Support for passing multiple app configurations through App Catalog >>

MaaS360 adds support for passing multiple app configurations using bundles within a bundle array. With this feature, administrators can define a maximum of 5 app restrictions for an app in the form of key and value pairs. Previously, MaaS360 allowed administrators to configure one app restriction for an app.

Analytics

Insights Advisor for Unified Endpoint Management >>

In this release, MaaS360 extends Insights Advisor functionality to UEM customers and provide insights about macOS and Windows devices that are missing critical OS patches. These Insights allow administrators to access all devices missing certain critical patches recommended by the Insights Advisor with a click of a button and initiate patch deployment to relevant devices in real-time.

Cloud Extender 2.93

Upgrade core Cloud Extender agent directly from Cloud Extender Configuration Tool >>

Cloud Extender version 2.93 release introduces enhancements to the Cloud Extender Configuration Tool where administrators can upgrade the Cloud Extender core to the latest version with a click of a button. The Cloud Extender Configuration Tool automatically checks for newer versions of the code and notifies administrators about the new core availability for download and install. The Cloud Extender core installer typically packages basic communication libraries and it is recommended to upgrade this core to the latest version to receive important security and functionality updates.

Use HTTPS URL for internet connectivity check >>

Cloud Extender version 2.93 release now supports the **Internet Connectivity** check on a HTTPS URL. This was previously an HTTP URL and was only used to check internet access and no other communication against this URL. Organizations might have to allow outbound HTTPS access against this new URL if it is being blocked for any reason.

Support for multiple S/MIME certificates from Active Directory >>

Cloud Extender version 2.93 release supports retrieval of all S/MIME encryption certificates from Active Directory, regardless of whether a matching certificate has expired. This allows end users to be able to read older messages encrypted with an older / expired S/MIME encryption certificate in MaaS360 Secure Mail.

Easy lookup of OU's from Corporate Directory during Cloud Extender Configuration >>

Enhancements have been made to the Cloud Extender configuration tool to simplify configuration of User Authentication and User Visibility modules. The tool now allows administrators to connect to Active Directory / LDAP and lookup Organization Units (OU's) and Distinguished Names (DN's) required for configuring them in Cloud Extender. User Search base, User and Group filters can now be selected from a pop-up screen instead of having to type them out during configuration.

Android 6.40 Release Summary

MaaS360 makes the Android app version 6.40 beta available in Play Store on 21 November 2018.

MaaS360 for Android app version 6.40 includes the following applications

- MaaS360 for Android core
- OEMs
- PIM
- Docs
- Secure Browser

MaaS360 for Android core

Deprecation Of SAFE Tags

Samsung will no longer be utilizing the SAFE language for security features. From 6.40 on the "SAFE" tag on the "Installed Services" page of the device view will be deprecated, and only the KNOX version will be displayed.

Support for additional Android Enterprise policies >>

MaaS360 adds support for additional Android Enterprise policies for Android devices running OS version 9 and above.

Enforcement of device enrollment for DO mode

MaaS360 enforces the device enrollment for all the Device Owner enrollment methods including the user-driven enrollments such as token-based and NFC bump. In the previous releases, MaaS360 introduced an option in the QR code and Zero-touch enrollment workflows to allow administrators to enforce the device enrollment.

Deprecation of Device Admin policies >>

When the Android upgrades its OS to version 10 in 2019, some of the Device Admin policies will be deprecated.

App wrapping enhancements >>

MaaS360 adds support for new configuration parameters to overcome issues during the app wrapping. Effective 10.71, MaaS360 allows administrators to enable multidex for Analytics-only (marked for collecting analytics data) apps.

One-stop shop for all Android enrollments >>

Maas360 adds Android Enrollment Wizard, a consolidated workflow for all Android enrollments - Device Admin, DO (Device Owner), and (PO) Profile Owner. The enrollment wizard displays interactive options to help you drill down to the Android enrollment method that suits your requirements. While this new feature greatly minimizes the time and efforts for the new customers, the existing Android enrollment menus are still available in the MaaS360 portal.

Biometric authentication support for Android 9 and above devices >>

MaaS360 enables biometric authentication support for Android devices running OS version 9 and above. With this support, a new authentication screen is displayed if the fingerprint authentication is enabled for the MaaS360 app.

MaaS360 agent behavior on expiration of MaaS360 account >>

When the MaaS360 account is terminated, the enrolled devices no longer report to the MaaS360 portal. A notification is sent to the devices to allow the users to remove the MDM control on the device.

NOTE

- Minimum version to create Knox Container: KNOX 2.0 & above devices
- Mobile Data Usage Feature in 6.40 release is being release as Beta. Please send feedback to MaaS360 Customer Support.

App Catalog

Support to deploy Private channel apps to App Catalog >>

MaaS360 now allows administrators to deploy the Private channel (managed) apps to the App Catalog. With this support, end-users can view and manage all Android apps (private, public, enterprise) in a centralized location. Previously, the Android Enterprise users had to install the private channel apps from the managed Google Play store.

Support to add Android Enterprise apps from managed Google Play account >>

MaaS360 embeds managed Google Play iframe in the App Catalog to allow the administrators to add and approve Google apps directly from the managed

Google Play store. In the previous releases, administrators had to add apps from the public Google Play store.

Support to edit app installation and update settings for Android enterprise apps >>

MaaS360 adds support to allow the administrators to edit the installation and update settings for Android enterprise apps. With this support, administrators can deploy the enterprise app updates to the devices that already have the primary version sideloaded through a third-party source (other than MaaS360). Requires MaaS360 for Android agent 6.40 and above.

OEMs

Support for additional MDM policies for Honeywell devices >>

MaaS360 adds support for additional MDM policies for Honeywell devices.

PIM

Support to propose a new meeting time >>

MaaS360 now allows attendees to propose a different time if the meeting invite conflicts with another meeting on their calendar. The feature also allows the organizers to see all proposed times for all attendees and change the meeting time to one of the proposed times. Note: The feature is only supported on Exchange 2016+ and Office365 servers that use the new ActiveSync 16.1 protocol.

Set the start date of calendar week and work week >>

MaaS360 adds support to set your own work days and when to start your work days and calendar days.

Docs

Distribution of documents to the device storage

MaaS360 adds support to distribute documents to the device storage through the Docs app. **Note**: The Storage permission must be enabled on the device.

Secure Browser

Cert-based authentication support >>

MaaS360 adds cert-based authentication support for Secure Browser, allowing the users to authenticate the webpages using the identity certificates.

iOS 3.70 Release Summary

MaaS360 makes the iOS app version 3.7 beta available to download/upgrade from the App Store on September 11, 2018.

The MaaS360 for iOS app version 3.7 includes the following applications:

- MaaS360 core app
- MaaS360 Secure Mail
- MaaS360 Docs
- MaaS360 Calendar

MaaS360 for iOS (core app) Enhancements

Redesigned Settings UI >>

MaaS360 revamps the Settings UI to granularly break down general and notification settings for Mail, Calendar, Contacts, and Tasks under separate screens. Previously, all the sections were available in different sections on the same screen. Also, the Logout option for shared devices is removed from User Info screen and added at the bottom of the Settings screen.

Deep links for MaaS360 enterprise app catalog >>

MaaS360 adds support for deep links, allowing the users to directly navigate to the detail view of an application in the enterprise app catalog by just tapping an URL from a different app. For example, IT staff can create and send a custom URL to the download page of a VPN application.

Support to update individual certificates on a device >>

MaaS360 now allows administrators to update a single certificate or multiple certificates on devices that are enrolled in the MaaS360 Portal that use the Persona policy. In the previous releases, if one certificate was expired/revoked, administrators had to regenerate all the certificates.

MaaS360 Secure Mail

Print action moved out of Reply menu >>

MaaS360 moves the Print action under the icon in the top right corner in the mail view. Previously, the Print action was a part of the Reply menu.

Support to restrict synchronization of email drafts >>

In the previous releases, MaaS360 added support for two-way synchronization of email drafts with the mail servers that support EAS (Exchange Activesync) protocol version 16 and above. In this release, MaaS360 adds support to disable the synchronization of drafts. Note: When the sync is turned off, the email drafts are removed from the MaaS360 app without deleting the drafts on the server. Users can turn on the draft sync anytime to resync drafts from the server.

Restriction on outgoing emails sent to external domains >>

MaaS360 adds support to allow administrators to restrict outgoing emails to corporate domains. Based on the type of restriction, the outgoing emails to external domains are blocked or a warning message is displayed.

Exchange ActiveSync 16.1 support >>

In the previous releases, MaaS360 added support for EAS (Exchange ActiveSync) protocol version 16. In this release, MaaS360 adds support for Exchange ActiveSync version 16.1. With the latest version, MaaS360 offers enhanced email and calendar features. Note: The upgrade will cause the emails, calendar, and contacts to resync, so those features will be unavailable for a brief period of time during the resync.

Support for custom mailto: links >>

MaaS360 adds support for custom mailto: links, allowing the users to activate the Secure Mail app from any of the apps for sending an email. When the users click the custom mailto: link, MaaS360 opens the New Message screen with the recipients, subject, and body text already filled in for them.

Support to manually download full message >>

MaaS360 now allows the users to manually download the full message when emails with broken links and missing CSS are received.

Support to send diagnostic logs to intended recipients >>

MaaS360 removes the hardcoded MaaS360 support email address from the MaaS360 for iOS app, leaving the **To** field open to the discretion of the users. With this support, users can forward the MaaS360 logs to administrators or the MaaS360 support team.

MaaS360 Docs

Support to access AD RMS-protected documents through multiple email accounts >>

MaaS360 adds support to access Active Directory Rights Management Services (AD RMS) protected documents through managed email accounts: primary email account, secondary email account, enrolled email account, or OneDrive/Office 365 SharePoint source. In the previous releases, the protected documents were accessed only through the primary email account.

MaaS360 Calendar

Support to respond to meeting invites without notifying the organizer >>

MaaS360 now allows users to respond to the meeting invites without notifying the organizer. Supported for all three actions: Accept, Maybe, Decline from both calendar and mail views. **Heads up**: When a user accepts/declines a meeting without sending a response, the meeting is recorded in the user's personal calendar, but the organizer is unaware of the response. Also, the attendance is not registered on the organizer's calendar, so the organizer cannot track those meeting responses.

Support to propose a new meeting time >>

MaaS360 adds support to allow users to propose a new meeting time if the meeting invitation conflicts with another meeting on their calendar. **Note**: Supported only for **Decline** and **Maybe** actions.

Support for custom recurrence pattern >>

MaaS360 Calendar now supports custom recurring patterns, allowing the users to create events with custom recurrence intervals. Previously, users had to select from the default recurring intervals. For example, users can create events such as repeat once in 26 weeks on Thursday or repeat every 88th day, instead of weekly or monthly.

Misc

32-bit architecture support deprecation >>

The MaaS360 iOS v3.7 app (currently in the App Store) will be the last version that will support 32-bit architecture.

Defect Fixes

Defect	Summary
32602	When a deep link is launched, the startup message **A new app is available. Click Continue to review details** is not displayed and the users are redirected to the web view of the app.
32332	The Failed Settings field in the device view is updated when users successfully log into their mail accounts. In the previous versions, the field was not updated on a successful login.
32226	The .ics file is not included in the acceptance notifications received by the organizer.
32132	The boundary distance is successfully tracked and the MaaS360 app successfully reports the location to the MaaS360 portal. Previously, due to a timing issue in the MaaS360 app, the location was not reported on some days.
32130	MaaS360 adds a new advanced property to turn on the *Mail settings > Accessibility* by default. Previously, when the Accessibility is off, the mail view is adjusted to fit the screen, thereby reducing the font size.
31954	MaaS360 calculates the location timestamp using the UTC/GMT calendar instead of device calendar.
31910	The brightness of the buttons on the PIN screen is increased when the contrast on the device is increased and the dark color is enabled.
31898	MaaS360 displays accurate unread email count. Previously, there was a discrepancy between the unread email count and actual unread emails.
31882	The MaaS360 for iOS app retrieves appropriate search results.
31694	The field size of the contacts is enhanced to avoid truncation. The contact names will now be truncated when the name exceeds three lines.
31654	The emails that consist Cyrillic script are successfully rendered in the Secure Mail.
31644	MaaS360 adds a new **Restrict Screenshot** setting in Persona policy > **WorkPlace** > **Security** > **Configure Data Protection** to allow administrators to disable screen sharing and screen recording. Note: This feature is only supported on mixed mode accounts. For more information, see Support for restricting the screen recording
31559	The alphanumeric password is successfully applied when a simple passcode is disabled in a persona policy. Previously, the error message **The passcode must not have ascending or descending characters** was displayed even though an alphanumeric password was provided.
31360	The calendar invites sync accurate date and time.
31163	The devices are successfully released from quarantine after the approval. Previously the devices were quarantined for hours.
31094	When a SharePoint is set up to connect the corporate resource, the connection is retained without the user having to re-configure Sharepoint access.
31075	The task badge count will show the count of overdue tasks from all folders and across all accounts. Previously, the count of overdue tasks plus new tasks was displayed.
30978	The inline images forwarded from the Secure Mail app are successfully displayed in the Notes app.

30602	MaaS360 retrieves search results from all contact folders irrespective of folder selection. Also, MaaS360 disabled retrieving results from the Recently Sent folder to avoid duplicates.
30598	When the MS Office files are opened, MaaS360 displays a toast message to allow the users to open the document in Secure Editor.
30578	When a calendar invite is created and successfully synced to the server, but if the sync is timed out, instead of creating a new invite entry MaaS360 removes the duplicate entry.
30211	MaaS360 removes the hardcoded MaaS360 support email address from the MaaS360 for iOS app, leaving the **To** field open to the discretion of the users. With this support, users can forward the MaaS360 logs to administrators or the MaaS360 support team. For more details, see Support to send diagnostic logs to intended recipients.
29969	MaaS360 displays accurate badge count for unread emails. Previously there was a mismatch between Outlook and MaaS360 Secure Mail.
29863	The document display name is displayed for the password-protected docs. Previously, a hashed name was displayed.
29353	MaaS360 adds support for custom mailto: links, allowing the users to activate the Secure Mail app from any of the apps for sending an email. When the users click the custom mailto: link, MaaS360 opens the New Message screen with the recipients, subject, and body text already filled in for them. For more information, see Support for custom mailto links.
28440	MaaS360 now allows the users to manually download the full message when emails with broken links and missing CSS are received. For more information, see Support to manually download full message.

Known Issues

Defect	Summary
31644	The support to restrict screen recording/sharing is limited to mixed mode customers. The feature is not supported on SPS accounts.
29353	When a user clicks an App Catalog deep link if an alert open in the core app, the UI gets cluttered.

iOS 3.80 Release Summary

MaaS360 will make iOS app version 3.8 beta available in iTunes on November 30, 2018.

The MaaS360 for iOS app version 3.8 includes the following features:

MaaS360 for iOS (core app) Enhancements

MaaS360 app for Apple Watch >>

MaaS360 releases its first version of Apple Watch app, allowing the users to manage emails and calendar on the go. With this new app, users can seamlessly view emails, respond to emails, and view calendar events. Note: This feature is not enabled by default. Contact the MaaS360 support team to enable this feature for your account. After you enable the MaaS360 app on Apple Watch, the content is automatically synced from your iOS device to the Apple Watch.

Custom suggested shortcuts for MaaS360 app >>

MaaS360 identifies a set of custom shortcuts for commonly performed tasks in Docs, Secure Mail, Document, and Assistant apps that you can add to the Siri app. Note: The feature is supported only on iOS version 12 and above and applicable only for primary accounts.

Calendar

Support for Work week view >>

MaaS360 adds support for the Work week view - the days that are spent working in a week. A general work week starts from Monday through Friday. If an organization has a non-traditional schedule, MaaS360 allows users to set their own work days. With this feature, MaaS360 displays only the events and meetings for the working days.

Support to edit imported calendar events >>

In the previous releases, MaaS360 added support to sync events from the native calendar to allow users to view personal and work events in the MaaS360 Calendar. The events that were imported from the personal calendar were available for read-only. In this release, MaaS360 allows users to edit and delete the personal events directly in the MaaS360 app without having to switch to the native calendar app. **Note**: The changes are automatically updated in the native calendar app.

Support to change the meeting time to proposed time >>

In the previous releases, MaaS360 added support to allow the attendees to propose a different time if the meeting invite conflicts with another meeting on their calendar. In this release, MaaS360 allows the organizers to see all proposed times for all attendees and change the meeting time to one of the proposed times. **Note**: The feature is only supported on Exchange 2016+ and Office365 servers that use the new ActiveSync 16.1 protocol.

Secure Mail

Granular notification groups >>

MaaS360 adds on top of iOS per-app notification grouping feature to provide a more granular approach for email and calendar notifications. With this feature, MaaS360 smartly stacks the notifications in the Notification Center based on the predefined conditions: VIP and high priority emails, meeting messages, all other emails, calendar meeting reminders, and pending task reminders. **Note**: The feature is supported only on iOS version 12 and above.

Email quick responses >>

MaaS360 adds support for quick responses, allowing the users to respond to the emails with the predefined responses when they are busy. The users can select from the existing response or create their own responses.

Contacts

Support for Homepage field

MaaS360 adds support for the Homepage field of type URL, allowing the users to provide a web address for a contact.

Misc

32-bit architecture support deprecation >>

The MaaS360 iOS v3.8 app has deprecated 32-bit architecture.